SONY
COMPUTER ENTERTAINMENT®

Sony Computer Entertainment America
919 East Hillsdale Blvd.
Foster City, California 94404-2175
650 655 8000
650 655 8001 Fax

May 26, 2011

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable G. K. Butterfield
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bono Mack and Ranking Member Butterfield:

Thank you for your letter of May 17, 2011, providing Sony with an opportunity to update our previous responses and to answer the Committee's follow-up questions. I would also like to take this opportunity to express my sincere gratitude to the committee for its appreciation of the gravity of the situation that Sony faced and, accordingly, allowing Sony to defer an appearance before the Committee. Sony was unable to appear before the Committee due to exigent circumstances. Sony was under attack, and it was critically important that our key personnel remain available and ready to address critical issues as our network and game service operations were preparing to come back on line.

To answer the Committee's questions I believe that it would be helpful to provide additional background information so that the Committee can better understand the nature and complexity of these events. Sony was the victim of multiple cyber attacks that occurred over a period of several weeks. Initially, Anonymous openly called for and carried out massive "denial of service" attacks against numerous Sony internet sites in retaliation for Sony Computer Entertainment America bringing an action in Federal Court to protect its intellectual property. The bulk of those attacks were targeted at services offered by Sony Network Entertainment America (SNEA) and Sony Online Entertainment (SOE). Many of the attacks lasted for several days. We now know that at some time during or shortly after those attacks, one or more highly skilled hackers infiltrated the servers of SNEA and SOE. The first indication that there was a problem was when several of SNEA's servers began to act in an unexpected manner. Four servers

were initially isolated as suspect. As similar abnormalities were discovered in other servers within the network system, the decision to shut down the entire system was made. This was done in an attempt to protect our customers' data. At the time we did not know the cause of the abnormalities or the extent of the intrusion. Until we had more information about what had occurred, it would have been imprudent to publicly speculate about the details of the attack.

Immediately after the network was shut down, forensic experts were called in to preserve evidence so that Sony could determine what had occurred. Unfortunately the need to capture and protect evidence through the "mirroring" process often conflicts with the equally important need to understand what occurred and the scope of a breach. Information security experts could not begin to understand what had happened, or the scope of the breach, until they had captured all the data on the affected servers. This takes time. More problematic, evidence shows that the hacker(s) took measures to cover their tracks in and out of the servers and to conceal what information they stole. Our forensic investigation is still ongoing and definitive answers remain elusive. As yet, we do not know who was responsible for the intrusion; nor do we know precisely the amount of information that was taken; nor do we know with certainty the number of users whose data was actually affected. These gaps in what we know are not for lack of trying by experts, but rather an unfortunate testament to the skill of those who perpetrated the attacks. Some aspects of the intrusion may never be known. To date, however, there is no evidence that credit card information was taken.

One final point before turning to your questions: we are very reluctant to release certain investigative information publicly because it is the subject of an ongoing criminal investigation, and because its disclosure could jeopardize the security of other network systems, not just our own. If the Committee wishes technical specifics, we would be happy to explore ways in which we could share this information with you – either under seal or in camera – if such means are available. In answering the Committee's questions, where appropriate I have noted these concerns. Turning to your questions:

1) **Has your investigation revealed any additional information on what customer information was specifically obtained, and whether the information was obtained from all accounts or a portion of the accounts?**

   We have information that suggests what the hacker was accessing and what the hacker may have downloaded, but we are unable to determine conclusively whether information was actually taken from all or just a portion of the user accounts. Accordingly, we believe it is appropriate for notification purposes to assume information could have been taken from any of the 77 million accounts, and we have notified each of our account holders using e-mail and/or public notices.

2) **When Sony representatives briefed our staff on May 3, 2011, they indicated that personal information from all 77 million accounts had been breached in some form. In your May 3, 2011 response to our letter you indicated not every piece of information in each account had been stolen, but that some personal information on all 77 million had been stolen. Has your investigation revealed what information was taken from each individual account? Do you have any additional information that would call for revising the number of affected accounts?**

To answer this question accurately it is necessary to distinguish between SNEA and SOE.

The 77 million user accounts referenced by our representatives referred to all of the SNEA customer accounts. Available evidence suggests that a database containing personal information for every account was accessed and that an attempt was made to take information from certain data fields in that database. We advised all of our customers in e-mails and on our website that we believed: *"an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID."* This list reflected the information we know the hacker accessed and was the data the hacker attempted to take off the servers. Unfortunately we cannot confirm whether the hacker was completely successful in taking all of that information off the servers, or just a subset of it; in an abundance of caution, Sony advised all of its customers that it believed that the data had been obtained.

On May 1, 2011, SOE discovered that customer data on its servers had also been accessed in a manner very similar to the SNEA intrusion. SOE gave notice of the breach to all of its customers. SOE had approximately 26.4 million user accounts containing user information.

3) **Has your investigation revealed how the breach occurred?**

We believe we know how the hacker gained access to each of the two networks, but the investigation is ongoing regarding other aspects of the criminal attack. As stated above, we believe that publically releasing these facts could jeopardize the ongoing investigation and potentially put other network systems at risk. We would be happy to explore a confidential and secure manner in which to outline this information to the Committee.

4) **Your initial reply to us on May 3 indicated the attack may have been coordinated and directed by the group of cyber criminals named 'Anonymous'. Have you identified those who are responsible for the breach, including any individual(s)**?

We have not yet identified the individual or individuals responsible for the actual intrusion and breach into our systems. We are continuing to work with the FBI to apprehend those responsible.

5) **When our staffs met on May 3, 2011, your representatives indicated Sony could not confirm whether credit card information had been breached but, at the time, there was no evidence to indicate that such information had been breached. Has your investigation revealed any additional information regarding whether credit card information was indeed taken.**

Based on the evidence available on May 3, 2011, Sony believed that no credit card data had been taken from PSN/Qriocity but could not rule it out. Since that time, no further forensic or circumstantial evidence has been discovered to suggest that any credit card data was taken. In addition, to date there have been no confirmed reports of credit card misuse or reports of an increase in fraudulent transactions resulting from this incident. Even so, our investigation is continuing.

6) **Sony discovered on May 1 that an additional breach of its network occurred. This breach reportedly involved approximately 25 million user accounts at Sony Online Entertainment .**

a. Was this breach the same as, related to, or unrelated to the Sony PlayStation Network breach? Have you identified the responsible party?

The timing, techniques, and methods used by the hacker suggest that the SOE breach was perpetrated by the same person or persons as the PlayStation Network breach. We have not yet identified the responsible party.

b. When did the breach occur? If there was a delay in the discovery of the Sony Online Entertainment breach, what was the reason for the delay?

Until May 1, 2011, SOE did not believe that any data had been taken from its databases, but access to the database appears to have occurred on April 16th and 17th, 2011. Upon learning that its databases had been breached, SOE made an announcement to its customers the following day. The investigation is continuing.

7) **What steps has Sony taken or does Sony plan to take to mitigate the effects of these breaches on its customers?**

Sony is making identity theft insurance available to customers in the United States. These customers are being offered a one year, $1 million identity theft insurance policy. Similar

programs will be offered in Canada and in the Latin American countries where such programs are available. In countries where insurance is not available, Sony is seeking to identify comparable programs to offer to its customers. In addition, while much of the PlayStation network is a free service, services on the PlayStation Network or Qriocity service that are fee based will be extended for the period of time that the service was down. For all of Sony's network customers, Sony is offering a "Welcome Back" package that provides several free offers including our Music Unlimited and PlayStation Plus services (for PlayStation owners) for a period of 30 days, along with a multitude of other free offerings.

8) **Regarding both the Sony PlayStation Network and the Sony Online Entertainment servers, you indicated in your May 3 response steps Sony is implementing to prevent future such breaches. Do you believe these additional security measures will prevent future breaches or illegal intrusions? Why did you not have these measures in place prior to the breach(es)?**

Sony took aggressive action to contain the intrusion and believes that its enhanced security measures should improve the security of these networks against attempted breaches in the future. We also recognize that no security system is absolutely foolproof, and changing conditions in the future can make a currently secure environment less secure: security is a never-ending battle of measures, counter-measures and counter-counter-measures against rapidly evolving and new threats. In light of this, SNEA and SOE now have an ongoing program of updating technology, continual testing of their security systems, review of external threats, and cooperation with law enforcement to provide a safe environment for customers. SNEA was in the process of putting in place several key security measures (as set out in my May 3 response) before the attacks occurred; SOE had already taken a variety of steps in a multi-layered approach to securing its network prior to the attack. In light of the sophistication of the attack, each company has made further refinements to its overall network security including new intrusion detection methods, policy changes, additional firewall protection, and more in-depth application testing prior to deployment.

9) **Did Sony have a policy in place at the time of either breach addressing data security and data retention practices? If not, why not? If so, what are those practices and does Sony plan any changes in its policies as a result of this breach?**

Sony has several policies addressing data security. Both companies were covered by the company's Global Information Security Policy, Global Information Security Standards, and the Global Basic Principles On Personal Information. Each company had its own privacy and IT security officers. In addition, SNEA and SOE are substantially building up their network security by increasing the number of technical measures they employ; for SNEA, the company has moved its data center to a more secure facility and, in light of this incident, SNEA and SOE are

reviewing their policies for scheduled inspection and updating of their sites. Moreover, both companies are conducting reviews on numerous fronts to help assure both procedural and substantive best practices going forward.

10) **In today's Wall Street Journal, Chief Executive Howard Stringer said Sony "can't guarantee the security of its videogame network... in the bad new world of cyber crime". Please explain what he meant, as well as the potential impact on consumers.**

Mr. Stringer sought to emphasize that no individual, corporation, or government entity, standing alone, can truly guarantee security in a world of very sophisticated hackers, cyber attacks, and cyber terrorism. Sony is implementing better and more robust security measures to protect our customers. But just as individuals and businesses have come to rely on multiple law enforcement agencies for physical protection, we believe the private sector will need the assistance and support of government and law enforcement to help secure e-commerce and IT systems to stay ahead of and curtail the activity of cyber criminals and cyber terrorists.

We hope this letter assists the Committee in answering the questions that it has posed.

Respectfully submitted,

for Kazuo Hirai

Kazuo Hirai
Chairman of the Board of Directors
Sony Computer Entertainment America LLC

cc: The Honorable Fred Upton
Chairman
U.S. House of Representatives
Committee on Energy and Commerce

The Honorable Henry A. Waxman
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce